PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347846
(43)Date of publication of application : 15.12.2000

(51)Int.Cl. G06F 9/06
G06F 13/00
H04Q 7/38

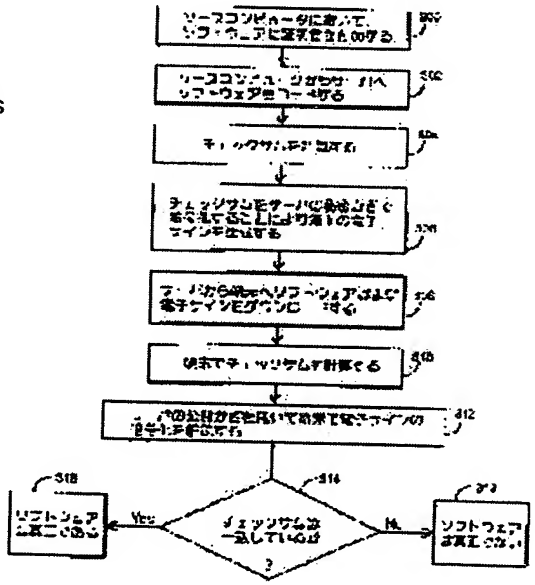
(21)Application number : 2000-063345
(22)Date of filing : 03.03.2000

(71)Applicant : NOKIA MOBILE PHONES LTD
(72)Inventor : PARKKINEN JUKKA

(30)Priority
Priority number : 99 990461 Priority date : 03.03.1999 Priority country : FI

(54) METHOD AND TELEPHONE SYSTEM FOR DOWNLOADING SOFTWARE FROM SYSTEM TO TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To confirm that software is downloaded from a proper server and produced by a proper software producer by comparing a first checksum with a second checksum and checking the intrinsicalness of the software in a terminal.
SOLUTION: A digital certificate for confirming the intrinsicalness of software to be transferred is added and the software is uploaded to a server (S300 and S302). By calculating and enciphering a checksum, an electronic sign is generated (S304 and S306). The required software is downloaded from the server to a terminal (S308). The checksum of the downloaded software and the added certificate is calculated and the intrinsicalness of the software is checked (S310). The enciphered electronic sign is deciphered while using a public key of the server (S312). The checksum, which is calculated by the server, obtained as a result of deciphering is compared with the checksum calculated by itself and the intrinsicalness is determined (S314).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－347846
（P2000－347846A）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ａ
					５５０Ｚ
	13/00	３５１		13/00	３５１Ｈ
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｍ

審査請求　未請求　請求項の数９　ＯＬ　外国語出願　（全 24 頁）

(21)出願番号　特願2000－63345(P2000－63345)

(22)出願日　平成12年３月３日(2000.3.3)

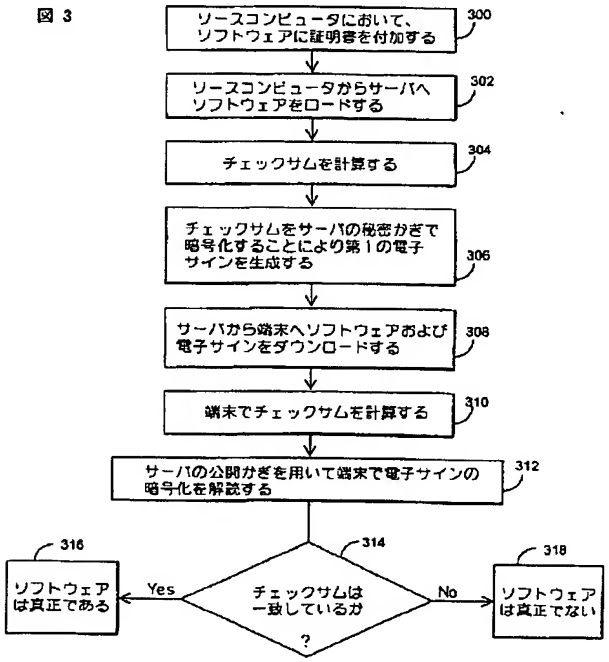
(31)優先権主張番号　９９０４６１
(32)優先日　平成11年３月３日(1999.3.3)
(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　590005612
ノキア　モービル　フォーンズ　リミティド
フィンランド国，エフアイエヌ－02150
エスポー，ケイララーデンティエ　４
(72)発明者　ユッカ　パルッキネン
フィンランド国，エフイーエン－90580
オウル，クラーセリンディエ　11　ベー
(74)代理人　100077517
弁理士　石田　敬　（外４名）

(54)【発明の名称】　サーバから端末にソフトウェアをダウンロードするための方法および電話システム

(57)【要約】
【課題】　サーバ（１２８）から端末（１００，１０２）にソフトウェアを、真正なソフトウェアであることを保証しながら、ダウンロードするための電話システムおよび方法に関する。
【解決手段】　この方法には、ソフトウェアおよびローダーの真正性を確認する証明書をソフトウェアに付加する段階、ソースコンピュータ（１３４）からサーバ（１２８）までソフトウェアをアップロードする段階、サーバ（１２８）から端末（１００，１０２）までソフトウェアをダウンロードする段階、が含まれる。ソフトウェアの真正性を確認する第１の電子サインがサーバ（１２８）においてソフトウェアに付加される。ソフトウェアがダウンロードされた後、ダウンロードされたソフトウェアから端末において第２の電子サインが生成され、ソフトウェアの真正性は第１の上記電子サインとその第２の電子サインとを比較することによってチェックされる。

図３



【特許請求の範囲】
【請求項１】　サーバ（１２８）から端末（１００，１０２）にソフトウェアをダウンロードするために、
ソフトウェア制作者およびローダーの真正性を確認する証明書を前記ソフトウェアに付加する段階と、
ソースコンピュータ（１３４）からサーバ（１２８）まで前記ソフトウェアをアップロードする段階と、
前記ソフトウェアおよび証明書のためのチェックサムを計算する段階と、およびサーバ（１２８）から端末（１００，１０２）まで前記ソフトウェアをダウンロードする段階と、を有する方法において、
前記ソフトウェアが端末にダウンロードされる前にサーバ（１２８）において前記ソフトウェアに対しそのソフトウェアの真正性を確認するチックサムを付加する段階と、
前記ソフトウェアがダウンロードされた後、ダウンロードされたソフトウェアから前記端末において第２のチェックサムを生成する段階と、および第１の前記チェックサムを前記第２のチェックサムと比較することにより前記端末において前記ソフトウェアの真正性をチェックする段階と、をさらに有してなることを特徴とする方法。
【請求項２】　前記ソフトウェアが実行されるときに、その真正性が常に端末（１００，１０２）においてチェックされることを特徴とする請求項１に記載の方法。
【請求項３】　前記ソフトウェアおよび証明書のために、サーバ（１２８）の秘密かぎを用いて暗号化される共通チェックサムを計算することによって、サーバ（１２８）において電子サインを生成する段階が含まれることを特徴とする請求項１に記載の方法。
【請求項４】　前記秘密かぎの暗号化が、サーバ（１２８）の公開かぎを用いて端末（１００，１０２）において解読されることを特徴とする請求項３に記載の方法。
【請求項５】　端末（１００，１０２）は、支払いカードが該端末のカード読取り装置（２０６）の中に挿入され、ユーザが１つのアプリケーションを選択したことを検出すること、および前記端末は、そのアプリケーションを実現するのに必要とされる前記ソフトウェアを該端末のメモリ内に発見できるか否かをチェックし、必要とされる該ソフトウェアについての情報を含むロード要求をサーバ（１２８）に送ること、および前記サーバは、前記端末に必要とされる前記ソフトウェアを送ること、および該端末は、そのソフトウェアをそのメモリ内に記憶すること、を特徴とする請求項１に記載の方法。
【請求項６】　複数の端末（１００，１０２）、および該端末の動作を監視および制御し、ソフトウェアおよびこれに付加された、証明書のためのチェックサムを計算するように構成されているサーバ（１２８）、
単数または複数のソフトウェアを記憶するための手段（２０４）を含む電話システムの端末とを含み、
サーバに対しソフトウェアをアップロードするように構成された単数または複数のソースコンピュータ（１３４）、前記サーバからソフトウェアをダウンロードするように構成された端末（１００，１０２）と、を含む電話システムにおいて、
前記サーバは、前記ソフトウェアが前記端末にダウンロードされる前に、該ソフトウェアの真正性を確認する第１のチェックサムを該ソフトウェアに付加するように構成されること、および前記ソフトウェアがダウンロードされた後、ダウンロードされたソフトウェアから第２のチェックサムを生成するように前記端末が構成されること、および該端末は第１の前記チェックサムを前記第２のチェックサムと比較することによってソフトウェアの真正性をチェックするように構成されること、を特徴とする電話システム。
【請求項７】　前記端末は、前記ソフトウェアが実行されるときにその真正性を常にチェックするように構成されることを特徴とする請求項６に記載のシステム。
【請求項８】　前記サーバは、前記ソフトウェアおよび証明書のために共通のチェックサムを計算することによって電子サインを生成し、該サーバの秘密かぎを用いて計算されたチェックサムを暗号化するように構成されることを特徴とする請求項６に記載のシステム。
【請求項９】　前記端末は、前記サーバの公開かぎを用いて前記電子サインの暗号化を解読するように構成されることを特徴とする請求項６に記載のシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数の端末と端末の動作を監視および制御する管理システムサーバとを備え、端末が単数または複数のソフトウェアを記憶するための手段を備える電話システムにおいて端末にサーバからソフトウェアをダウンロードするための方法に関する。
【０００２】
【従来の技術】無線電話システムが益々一般的になりその受信地域が拡大するにつれて（システムは往々にして固定回線電話接続により実現されるシステムに置き換わり）、セルラー無線システムといった無線電話システムを支援する電話ネットワークを開発することが必要となってきた。かかる電話は、例えば固定回線電話接続が存在しない地域または、固定ネットワークへの接続が容易に利用可能でない場所例えば移動車両内に端末が置かれる利用分野において必要とされる。本発明は、特に、セルラー無線システムを用いて実現されるシステムに適用することができる。
【０００３】関連するシステムおよび端末としては、公衆電話、いわゆるＷＬＬ（wirelesslocal loop）端末、ＰＯＳにおける支払い端末およびカードと銀行との間の送金を支援するスマートカード端末とがある。現行の端末における機能は、大部分がさまざまなタイプのソフト

ウェアを用いて実現される。端末は、プロセッサおよび必要なソフトウェアを記憶するメモリを具備する。ユーザが機能を選択したとき、ソフトウェアはメモリから読み出され、実行される。端末を設計するにあたっては、機能の数と利用可能なメモリ容量の間の妥協が必要であった。コスト上の理由から、端末内のメモリのサイズを無限に増大させることはできず、従ってメモリは機能の数を制限する。

【０００４】ここで一例として、無線システムを用いて実現される公衆電話システムについて検討する。このシステムは、各々が無線経路で基地局と通信する複数の公衆電話からなる。無線経路および基地局に対し、公衆電話として機能する端末はいかなる形であれ従来の加入者端末から逸脱するものではない。支払いの徴収については、この公衆電話は、標準的に支払いカード読取り装置でありうる徴収装置を備える。さまざまなタイプのクレジットカード、リロード可能な支払いカード、銀行カードといったように数多くの異なる支払いカードが利用可能である。さらに、カードのタイプは、カードメーカーおよびカード提供会社に応じて異なり、１つの同じカードについて異なる設備を選択することが可能である。各カードタイプは、そのカードを支援するソフトウェアすなわちカードアプリケーションが端末に備わっていることを必要とする。このカードアプリケーションは、カードを制御しかつ支払いといった取引を実行するため、端末のユーザインタフェースに必要なルーチンを含んでなる。

【０００５】

【発明が解決しようとする課題】カードを読取る端末のメモリ内に全てのカードタイプを支持するカードアプリケーションを記憶させるためには、非常に大きなメモリが必要であり、そのため端末は高価なものとなる。その上、端末に対し新しいカードアプリケーションを付加するには、機器全体のソフトウェアをハードウェアメンテナンスにおいて交換することが必要となる。

【０００６】公衆電話に関係するこれらの問題に類似した問題にはまた、支払いカードが読取られるその他の無線装置、例えば、銀行口座から支払いカードへ電子通貨をロードできるようにするリローディング装置にも影響を及ぼすということもある。上述の問題を解決するためには、必要な場合にネットワークを通してソフトウェアをダウンロードしかくして端末のメモリを最適な形で利用できるようにすることが可能であれば有利である。そのカードに対応するソフトウェアをもたない端末にカードが挿入されたときに、端末は、予め定められたサーバからネットワークを通してそのメモリに必要なソフトウェアをダウンロードすることができる。

【０００７】しかしながら、この方法には欠点がある。ネットワークからダウンロードされたソフトウェアの使用には、考慮に入れなくてはならない危険性が関与している。つまりダウンロードされるべきソフトウェアが完全なものであり、例えばソフトウェアウイルスまたはその他の有害な要素を含有していないことが重要である。また、ソフトウェアが適正なサーバからダウンロードされ、適正なソフトウェア制作者によって作られていることを確認することができるということも重要である。不良ソフトウェアは、意図していない呼および誤ったアドレスへの取引といったような、端末内の機能不良をひきおこす可能性がある。

【０００８】

【課題を解決するための手段】従って本発明の目的は、上述の問題を解決できるように、方法およびその方法を実現する装置を提供することにある。これは、サーバから端末へソフトウェアをダウンロードするための方法において、ソフトウェア制作者およびローダーの真正性を確認する証明書をソフトウェアに付加する段階、ソースコンピュータからサーバまでソフトウェアをアップロードする段階、ソフトウェアおよび証明書のためのチェックサムを計算する段階、およびサーバから端末までソフトウェアをダウンロードする段階、を含んでなる方法を用いて達成される。本発明の方法はさらに、ソフトウェアが端末にダウンロードされる前にサーバにおいてソフトウェアに対しそのソフトウェアの真正性を確認するチェックサムを付加する段階、ソフトウェアがダウンロードされた後ダウンロードされたソフトウェアから端末において第２のチェックサムを生成する段階、および第１の前記チェックサムをその第２のチェックサムと比較することにより端末においてソフトウェアの真正性をチェックする段階、を含んでなる。

【０００９】本発明はさらに、複数の端末と端末の動作を監視および制御し、ソフトウェアおよびそれに付加された証明書のためのチェックサムを計算するように構成されているサーバ、単数または複数のソフトウェアを記憶するための手段を含む電話システムの端末を含み、サーバに対しソフトウェアをアップロードするように構成された単数または複数のソースコンピュータを含み、端末がサーバからソフトウェアをダウンロードするように構成された電話システムにも関する。本発明の電話システムにおいては、サーバは、ソフトウェアが端末にダウンロードされる前に、ソフトウェアの真正性を確認する第１のチェックサムをソフトウェアに付加するように構成されており、端末は、ソフトウェアがロードされた後、ダウンロードされたソフトウェアから第２のチェックサムを生成するように構成されており、かつ該端末は第１のチェックサムを第２のチェックサムと比較することによってソフトウェアの真正性をチェックするように構成されている。

【００１０】従属クレームは、本発明の好ましい実施形態に関する。本発明の方法およびシステムは、複数の利点を提供する。本発明の解決法によると、ソフトウェア

が安全であり、安全なソースコンピュータからサーバへとそれがアップロードされることを保証するのが容易である。本発明は、ソフトウェアの真正性を確実にするためディジタルサインを利用する。対応する方法は、これまで、Ｅメール伝送に関連してのみ適用されてきたものである。

【００１１】

【発明の実施の形態】以下、本発明について、好ましい実施形態と関連して、添付図面を参照しながらより詳細に説明する。以下では、一例としてディジタルＧＳＭ移動体通信システムに適用することによって実現される公衆電話システムをもとにして、本発明について説明するが、本発明はこの例に制限されるものではない。本発明の解決法は、任意のその他の技術を用いて実現され、ソフトウェアアプリケーションを用いて動作させられる機能を含む端末を備える電話システムに応用すべく修正可能であるということは明白である。

【００１２】図１は、セルラー無線ネットワーク内で実現された公衆電話システムの構造を例示している。このシステムは、各々無線経路１０４～１０６を介して基地局（ＢＴＳ）１０８～１１０に接続されている複数の公衆電話（ＰＰ）１００～１０２を備える。無線経路または基地局については、公衆電話として動作する端末はいかなる形であれ、従来の加入者端末から逸脱するものではない。基地局１０８～１１０は、標準的には、光ケーブル、銅ケーブルまたはリンク接続を用いて実現可能な伝送ライン１１２～１１４を介して、複数の基地局を制御する基地局制御装置１１６～１１８に接続されている。基地局制御装置１１６～１１８の方はというと、これらは伝送ライン１２０～１２２を介して、基地局制御装置の動作を制御し端末から固定ネットワークへまたはセルラー無線システムのその他の部分に伝送ライン１２６を通して呼を伝送する移動通信交換局（ＭＳＣ）１２４に接続されている。

【００１３】公衆電話システムはさらに、公衆電話１００～１０２の動作を制御および監視する管理システムサーバ（ＰＭＳ）１２８を備える。一例としては使用されたＧＳＭシステムにおいては、公衆電話システムの制御機器サーバ１２８が、例えば、それ自体ＧＳＭセルラーネットワークおよびその移動交換局に接続されているショートメッセージセンタ（ＳＭ＿ＳＣ）１３２に、Ｘ．２５インタフェース１３０を介して接続されている。セルラー無線システムについての上述の説明はかくしてＧＳＭシステムに関するものであるが、その他のシステムもその細部が上述の説明から変更したものであれ、基本的な構造には差異が全くないということは明白である。またＧＳＭシステムにおいては、公衆電話システムの制御機器サーバ１２８をモデムといった他の従来技術の方法を利用することによりセルラー無線システムに接続することによって、ショートメッセージセンタ無しで公衆電話システムを実現することが可能であるという点に留意すべきである。

【００１４】本発明のシステムはさらに、端末内で使用されるソフトウェアの制作者のコンピュータといったようなソースコンピュータ１３４を備える。ソースコンピュータ１３４は、通信ネットワーク１３６例えばインターネットまたは私設ネットワークを介してサーバ１２８に接続される。サーバおよびソースコンピュータは共に、必要とされる電子通信特性および適切なソフトウェアを有するコンピュータハードウェアとして実現され得る。

【００１５】図２は、本発明のシステムによる公衆電話の好ましい実施形態の一例を示す。本発明の公衆電話はセルラー無線トランシーバ（ＭＳ）２００および２線接続(two-wire connection) 無しでこのトランシーバ２００に対する直接接続２０２を有する制御ユニット（ＣＰＵ）２０４を備える。本発明の端末はさらに、制御ユニット２０４に接続された徴収手段２０６を備える。アプリケーションに応じて、徴収手段は、テレホンカード、クレジットカードまたはスマートカードを支払い手段として受入れることができる。端末は、標準的には所望の電話番号をダイヤルするためのダイヤリング手段（ＫＥＹＢ）２１０、表示ユニット（ＤＩＳＰ）２０８およびイヤホン２１２も備えている。端末はまた、スピーカ２１６およびマイクロホン２１８を備えハンズフリー機能を可能にする手段２１４、および必要な増幅器をも含むことができる。望ましい場合には、上述のコンポーネントのうちの一部または全てを直接トランシーバユニット２００内に組込んでもよいし、あるいは、構造的にはできれば同じケーシング内ではあるもののこれらを別々の手段として実現することも可能である。

【００１６】トランシーバユニット２００の機能は、必要な場合に、呼を伝送できるように基地局に対する無線接続を提供することにある。ユニット２００はまた、無線経路および呼の維持に関する全てのオペレーション（通常は移動電話により行われるもの）をも処理する。制御ユニット２０４の機能は、公衆電話を制御することにある。制御ユニットは標準的にマイクロプロセッサ、固定されかつ再プログラミング可能なメモリ回路、多重化手段およびスイッチを備える。制御ユニットは、機器内に含まれているその他のユニットの動作を制御し、発生した呼を記録し、課金の処理をする。公衆電話の動作パラメータは通常制御ユニットのメモリ内に記憶されている。かかる電話特定パラメータとしては、電話番号、発生した呼に関する料金データ、電話の表示上の言語選択肢および音量などがある。本発明で説明されている進歩性のある特徴を除いて、制御ユニットの動作は、基本的に、先行技術の公衆電話の制御ユニットの動作と異ならない。

【００１７】端末構造の細部もまた、端末の使用目的に

応じて上述の説明から変更する可能性がある。例えば、端末がＰＯＳで使用される支払い端末である場合、装置は必ずしもマイクロホンまたはスピーカといったようなオーディオ部品を含むわけではない。最も単純なものの場合、端末は、互いに構造的に組込み可能なセルラー無線トランシーバユニット、制御ユニットおよび徴収手段を備えるが、これらに代えて、例えば呼の支払いまたは購入取引の間一時的に接続される互いに着脱可能な構成要素であってもよい。

【００１８】端末により必要とされるソフトウェアは、制御ユニット２０４のメモリ内に記憶される。当該ソフトウェアとしては、ソフトウェアまたはさまざまな支払いカードのオプションにより必要とされるカードアプリケーションが含まれる。カードアプリケーションには、カードを制御したり支払いといったカード取引を実施するための端末のユーザインタフェースに必要とされるルーチンが含まれる。

【００１９】次に、図３に示したフローチャートを参照しながら、本発明の方法について検討する。前述の通り、本発明のシステムは、必要な場合にシステムサーバから端末にソフトウェアをダウンロードすることを可能にする。ソフトウェアの真正性を保証するためには、ソフトウェアが、真正性が確認済みのソースからサーバに対しアップロードすることのみ可能であることが重要である。本発明の解決法においては、各々のソフトウェア提供者はかくして、ソフトウェア提供者またはソフトウェアをサーバに対しアップロードする提供者のコンピュータ（以下ソースコンピュータと称す）を識別することを可能にする特定のディジタル証明書の提供を受ける。この証明書は、端末メーカーといったような第三者によって付与される。

【００２０】図３のステップ３００においては、ソフトウェア制作者は、サーバに転送されるべきソフトウェアに対しその真正性を確認するディジタル証明書を付加する。ステップ３０２では、ソフトウェアは、例えばインターネットまたはその他のリンクを介して、この例では公衆電話システムのサーバであるネットワークサーバに対し、ソフトウェア制作者のソースコンピュータからアップロードされる。好ましい実施形態においては、サーバは、ダウンロードに関連してソースコンピュータの証明書をチェックする。

【００２１】ソフトウェアが端末にダウンロードされるとき、そのソフトウェアが、既にネットワークに接続されている妨害者からではなく予め合意された公式のサーバからダウンロードされることも不可欠である。従って、ソフトウェアの出所をソフトウェアから確認できることが必要である。この目的のため、ソフトウェアには、サーバにおいて、電子サインが備えられ、このサインはステップ３０６においてソフトウェアに付加される。本発明の好ましい実施形態においては、電子サインは、ソフトウェアおよび証明書についてステップ３０４でチェックサムを計算し、ステップ３０６で好ましくは暗号化を用いて、それによりいかなる部外者により合計がこわされないよう予防することにより、ソフトウェアにそのチェックサムを付加することによって生成される。チェックサム自体は、当業者にとっては公知の方法を適用することによって計算することができる。暗号化を実現する１つの方法は、公開かぎおよび秘密かぎ暗号化方法を使用することである。電子サインは、部外者が知らないサーバの秘密かぎを用いることによってステップ３０６でサーバにおいてソフトウェアに付加される。暗号化された情報はこのとき、端末において公開かぎを用いることにより解読され得る。本発明の解決法においては、当業者にとって公知の暗号化方法を使用することができる。

【００２２】ステップ３０８では、端末は、サーバから必要とされているソフトウェアをダウンロードする。端末は、ソフトウェアをダウンロードした後、サーバにおいてと同様に、ダウンロードされたソフトウェアおよびそれに付加された、証明書のチェックサムを計算することによって、ステップ３１０でソフトウェアの真正性をチェックする。端末は次に、ステップ３１２でサーバの公開かぎを使用することによりサーバにおいてソフトウェアに付加された暗号化された電子サインを解読する。解読の結果、サーバにて計算されたチェックサムが得られる。端末は、ステップ３１４で、自ら計算したチェックサムと、サーバにて計算されたチェックサムを比較し、この比較の結果により、端末は真正性について決定を下すことが可能となる。チェックサムが一致した場合、ソフトウェアは真正である（ステップ３１６）が、チェックサムが一致しない場合には、ソフトウェアのソースは真正でなく（ステップ３１８），ソフトウェアを使用に供することはできない。

【００２３】次に、ソフトウェアの前述のダウンロードを実行することのできない状況の一例について検討する。これは、図４および図５のフローチャートに例示されている。ステップ４００において、ユーザは端末のカード読取り装置２０６内にカードを挿入した。ステップ４０２では、端末は、カードの異なる機能、例えば内含されているあらゆるクレジットカードのオプションについてチェックする。複数の選択肢が利用できる場合、ユーザは、使用されるべき機能を選択することになる。ルーチンは次にステップ４０６に進みここで、選択された機能により必要とされるアプリケーションが端末のメモリ内に含まれているか否かをチェックする。アプリケーションは、ある特定の時にそのメモリ内で利用可能なアプリケーションの記録を保持する。そのアプリケーションがメモリ内にある場合、それをステップ４０８で開始することができる。

【００２４】そのアプリケーションが端末のメモリ内に

ない場合、ルーチンはステップ４１０まで進み、アプリケーションが管理システムのサーバ内にあるか否かをチェックする。サーバからダウンロードされ得るアプリケーションについての情報は、端末内に記憶されてもよいし、あるいは端末がサーバからその情報を要求することもできる。アプリケーションが管理システムから発見できない場合、その機能はステップ４１２で拒絶され、カードが複数の機能を含むことを条件として、ユーザは新しい機能を与えるよう求められる。

【００２５】アプリケーションが管理システムのサーバ上にある場合、端末はステップ４１４において、アプリケーションにより必要とされるメモリ量をたずねる。端末は次にステップ４１６において、アプリケーションにより要求されたメモリ量が使用可能であるか否かをチェックする。充分なメモリが使用可能でない場合、メモリから除去すべきアプリケーションが選定され、新しいアプリケーションのためにメモリを解放すべく、ステップ４１８で除去される。端末はユーザに、除去すべきアプリケーションを選択させることもできるし、あるいは、端末が予め定められた基準に基づいて決定を下すこともできる。１つの基準は、最近使用されたアプリケーションを保持し、最も長い間使用されずにきたアプリケーションを除去することである。

【００２６】このとき端末は、ステップ４２０においてサーバに対し、アプリケーションが置かれるべき未使用のメモリ領域について情報を与える。例えば、端末は、アプリケーションのために利用可能となるメモリ領域を通知することができる（図３の３１２）。管理システムのサーバはステップ４２２で、端末によって通知されたメモリ領域に対し、アプリケーションをダウンロードする。そして、このアプリケーションは、ステップ４２４においていつでも使用されうる状態にある。

【００２７】もう１つの別の実施形態においては、管理システムのサーバは、端末のメモリ内へのアプリケーションの挿入を制御せず、ただ単にアプリケーションを端末に伝送し、この端末が次にそのアプリケーションをそのメモリ内に入れる。支払いカードアプリケーションに加えて、ダウンロード可能なソフトウェアは、タイムテーブル情報またはチケットといった電子形態で転送される機能を含むことができる。

【００２８】本発明の端末に関連する方法ステップは有利には、端末の制御ユニット２０４においてソフトウェアにより実現され得る。この方法が必要とする管理システムのサーバに対する接続は、有利には、データ呼接続（data call connection）を用いて提供され得る。データ呼というのは、ディジタル無線ネットワーク内で利用可能な呼のタイプである。これは、アナログシステムにおけるモデム接続に対応する。

【００２９】管理システムのサーバにおいておよびソフトウェア制作者のソースコンピュータ内においては、本発明の機能は、有利にはソフトウェアを用いて実現可能である。本発明は以上で、添付図面に示す例を参照しながら説明されているものの、本発明がそれに制限されるものではなく、特許請求の範囲に開示されている進歩性のある考え方の範囲内で数多くの形で変形しうるものであることは明白である。

【図面の簡単な説明】

【図１】本発明の電話システムの構成を示す図である。

【図２】本発明によるシステムの端末の構成を示すブロック図である。

【図３】本発明の方法を示すフローチャートである。

【図４】ソフトウェアのダウンロードを示すフローチャート（その１）である。

【図５】ソフトウェアのダウンロードを示すフローチャート（その２）である。

【符号の説明】

１００～１０２…公衆電話
１０４～１０６…無線経路
１０８～１１０…基地局
１１６～１１８…基地局制御装置
１２４…移動通信交換局
１２８…管理システムサーバ
１３０…インタフェース
１３２…ショートメッセージセンタ
１３４…ソースコンピュータ
２００…セルラー無線トランシーバユニット
２０４…制御ユニット
２０６…徴収手段

【図１】

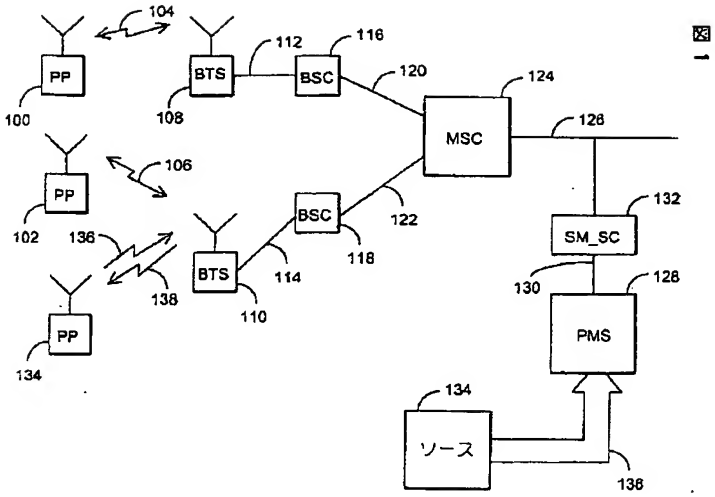

PP
100
104
BTS
108
112
BSC
116
120
MSC
124
126
PP
102
106
BSC
118
122
132
SM_SC
136
BTS
114
110
138
130
128
PMS
PP
134
134
ソース
136

図１

【図２】

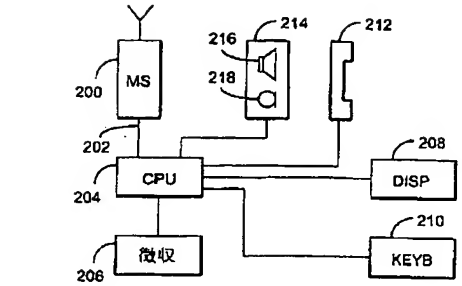


図 2
MS
200
216
214
218
212
202
CPU
204
208
DISP
210
KEYB
微収
206

【図３】

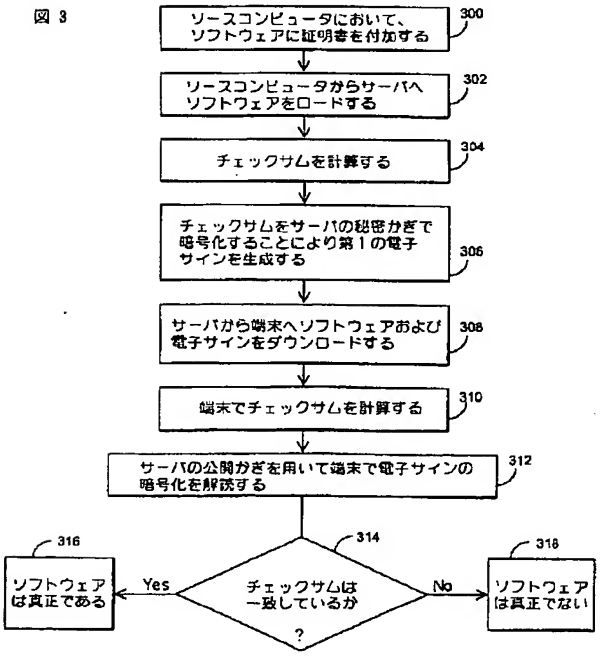


図 3
ソースコンピュータにおいて、ソフトウェアに証明書を付加する
300
ソースコンピュータからサーバへソフトウェアをロードする
302
チェックサムを計算する
304
チェックサムをサーバの秘密かぎで暗号化することにより第１の電子サインを生成する
306
サーバから端末へソフトウェアおよび電子サインをダウンロードする
308
端末でチェックサムを計算する
310
サーバの公開かぎを用いて端末で電子サインの暗号化を解読する
312
チェックサムは一致しているか
?
314
Yes
No
ソフトウェアは真正である
316
ソフトウェアは真正でない
318

【図４】

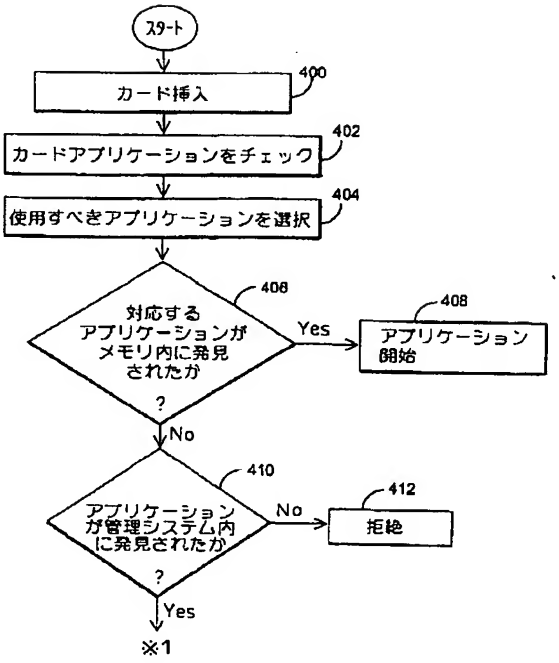


図 4
スタート
カード挿入
400
カードアプリケーションをチェック
402
使用すべきアプリケーションを選択
404
対応するアプリケーションがメモリ内に発見されたか
?
406
Yes
アプリケーション開始
408
No
アプリケーションが管理システム内に発見されたか
?
410
No
拒絶
412
Yes
※1

【図５】

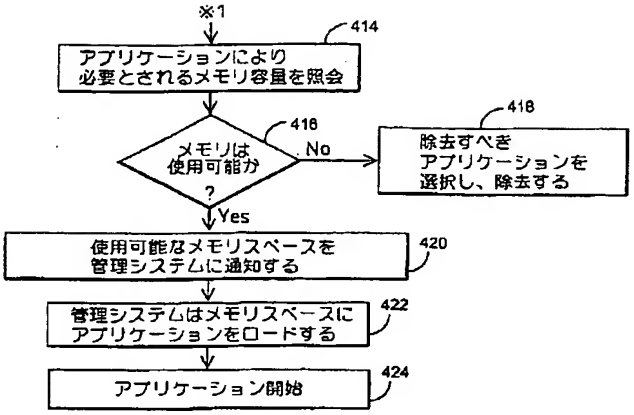

※1
414
アプリケーションにより
必要とされるメモリ容量を照会
416
メモリは
使用可能か
?
No
418
除去すべき
アプリケーションを
選択し、除去する
Yes
使用可能なメモリスペースを
管理システムに通知する
420
管理システムはメモリスペースに
アプリケーションをロードする
422
アプリケーション開始
424

図5

【外国語明細書】

1. TITLE OF THE INVENTION

METHOD FOR DOWNLOADING SOFTWARE FROM SERVER TO TERMINAL AND TELEPHONE SYSTEM

2. DETAILED DESCRIPTION OF THE INVENTION

The invention relates to a method for downloading software from a server to a terminal in a telephone system comprising a plural number of terminals and a management system server that monitors and controls the operation of the terminals, a terminal of the system comprising means for storing one or more software.

As radio telephone systems become increasingly common and their coverage areas grow - the systems often replacing those implemented by fixed line telephone connections - it has become necessary to develop telephone networks supporting radio telephone systems such as cellular radio systems. Such telephones are needed, for example, in areas where fixed line telephone connections do not exist, or in applications in which the terminal is in a place, for example in a moving vehicle, where connection to a fixed network is not easily available. The present invention can be applied particularly to systems implemented by means of cellular radio systems.

The systems and terminals involved include pay phones, so-called WLL (wireless local loop) terminals, payment terminals at points of sale and smart card terminals supporting transfer of money between a card and a bank.

The functions in current terminals are to a large extent implemented by means of various types of software. The terminal comprises a processor and memory into which the necessary software is stored. When the user selects a function, the software is read from the memory and carried out. In the designing of terminals, a compromise between the number of functions and the available memory capacity has been necessary. Due to reasons of cost, the size of the memory in the terminals cannot be infinitely increased, therefore the memory limits the number of the functions.

Let us study, by way of example, a pay phone system implemented by means of a radio system. The system comprises a plural number of pay phones, each communicating with base stations over a radio path. For the radio path and the base station, the terminals functioning as pay phones do not deviate in any way from conventional subscriber terminals. For collection of payments, the pay phones comprise a collection device that can typically be a payment card reading device. Numerous different payment cards are

available, such as different types of credit cards, reloadable payment cards, bank cards, etc. In addition, the card types vary according to the card manufacturer and the company offering the card, and different facilities can be selected for one and the same card. Each card type requires the terminal to be provided with software supporting the card, i.e. a card application. The card application comprises the routines required for the terminal's user interface, for controlling the card and for performing a transaction, such as a payment.

To have card applications supporting all card types stored into the memory of a terminal reading a card would require such a large memory that the terminal would be expensive. Furthermore, the adding of new card applications to the terminal would require the software of the entire equipment to be changed at hardware maintenance.

Problems similar to those relating to pay phones also affect other wireless devices in which payment cards are read, such as reloading devices allowing electronic money to be loaded from a bank account to a payment card.

To solve the above problem, it is advantageous if software can be downloaded through the network when necessary, thereby allowing the terminal's memory to be optimally utilized. When a card is inserted into a terminal which does not have software corresponding to the card, the terminal can download the needed software to its memory through the network from a predetermined server.

This method has, however, its shortcomings. The use of software downloaded from a network involves risks that must be taken into account. It is important that the software to be downloaded is flawless and does not contain software viruses, for example, or other harmful elements. It is also important to be able to verify that the software is downloaded from the correct server and that it is manufactured by the correct software manufacturer. A defective software can cause malfunction in the terminal, such as unintended calls and transactions to wrong addresses.

An object of the invention is therefore to provide a method and an apparatus implementing the method so as to allow the above problems to be solved. This is achieved with a method for downloading software from a server to a terminal, the method comprising the steps of attaching to the software a

certificate confirming the authenticity of the software manufacturer and the loader: downloading the software from a source computer to the server; calculating a check sum for the software and the certificate; and downloading the software from the server to the terminal. The method of the invention further comprises the steps of adding the check sum confirming the authenticity of the software to the software at the server before the software is downloaded to terminals; generating a second check sum at the terminal from the downloaded software, after the software has been downloaded; and checking the authenticity of the software at the terminal by comparing the first check sum with the second.

The invention further relates to a telephone system comprising a plural number of terminals and a server monitoring and controlling the operation of the terminals, the server being arranged to calculate a check sum for the software and the certificate attached to the software; a terminal of the telephone system comprising means for storing one or more software, and the system comprising one or more source computers arranged to upload software to the server, the terminals being arranged to download the software from the server. In the telephone system of the invention the server is arranged to attach to the software a first check sum confirming the authenticity of the software before the software is downloaded to the terminals, and a terminal is arranged to generate a second check sum from the downloaded software, after the software has been loaded, and that the terminal is arranged to check the authenticity of the software by comparing the first check sum with the second.

The dependent claims relate to preferred embodiments of the invention.

The method and system of the invention provide several advantages. With the solution of the invention it is easy to ensure that the software is safe and that it is uploaded to the server from a safe source computer. The invention employs digital signature to ensure the authenticity of the software. Corresponding methods have earlier been applied only in connection with electronic mail transmissions.

3. BRIEF DESCRIPTION OF THE DRAWINGS

In the following the invention will be described in greater detail in connection with preferred embodiments and with reference to the accompanying drawings, in which

Figure 1 is a diagram illustrating a structure of a telephone system of the invention;

Figure 2 is a block diagram illustrating a structure of a terminal of a system according to the invention;

Figure 3 is a flow chart illustrating a method of the invention; and

Figure 4 is a flow chart illustrating the downloading of software.

In the following the invention will be described, by way of example, with reference to a pay phone system implemented by applying a digital GSM mobile phone system, the invention not being, however, limited to the example. It is apparent that the solution of the invention can be modified to apply to telephone systems implemented by means of any other technology and comprising terminals which include functions operated by means of software applications.

Figure 1 illustrates a structure of a pay phone system implemented in a cellular radio network. The system comprises a plural number of pay phones 100-102, each connected via a radio path 104-106 to base stations 108-110. For the radio path or the base station, terminals operating as pay phones do not differ in any way from conventional subscriber terminals. The base stations 108-110 are typically connected to base station controllers 116-118, each controller controlling a plural number of base stations, via transmission lines 112-114 which can be implemented by means of optical cables, copper cables or link connections. The base station controllers 116-118, in turn, are connected via transmission lines 120-122 to a mobile services switching centre 124 which controls the operation of the base station controllers and transmits calls from the terminals to a fixed network or to other parts of the cellular radio system via transmission lines 126.

The pay phone system further comprises a management system server 128 which controls and monitors the operation of the pay phones 100-102. In the GSM system used as an example, a control equipment server 128 of the pay phone system is connected via an X.25 interface 130, for example,

to a short message centre 132 which is, in turn, connected to GSM cellular networks and their mobile switching centres. The above description of the cellular radio system thus relates to the GSM system, but it is obvious that although the details of other systems vary from the above description, there are no essential structural differences. It should be noted that also in the GSM system the pay phone system can be implemented without the short message centre, by connecting the control equipment server 128 of the pay phone system to the cellular radio system by employing other prior art methods, such as a modem.

The system of the invention further comprises a source computer 134, such as a computer of the manufacturer of the software used in the terminals. The source computer 134 is connected to the server 128 via a telecommunications network 136, such as the Internet or a private network. Both the server and the source computer can be implemented as computer hardware having the required telecommunications characteristics and the appropriate software.

Figure 2 illustrates an example of a preferred embodiment of a pay phone according to the system of the invention. The pay phone of the invention comprises a cellular radio transceiver 200 and a control unit 204 which has a direct connection 202 to the transceiver 200 without a two-wire connection. The terminal of the invention further comprises a collection means 206 connected to the control unit 204. Depending on the application, the collection means can accept phone cards, credit cards or smart cards as means of payment. The terminal typically also comprises a dialling means 210 for dialling the desired telephone number, display unit 208 and an earpiece 212. The terminal can also comprise means 214 allowing a hands free facility, the means comprising a speaker 216 and a microphone 218, and the necessary amplifiers. If desired, some or all of the above components can be directly integrated into the transceiver 200, or they can be implemented as separate means, although structurally possibly within the same casing.

The function of the transceiver unit 200 is to provide, when necessary, a radio connection to a base station to allow a call to be transmitted. The unit 200 also takes care of all operations (usually carried out by a mobile phone) concerning the maintenance of the radio path and the call.

The function of the control unit 204 is to control the pay phone. The control unit typically comprises a micro processor, fixed and reprogrammable

memory circuits, multiplexing means and switches. The control unit controls the operations of other units included in the equipment, registers placed calls and takes care of debiting. The operational parameters of the pay phone are usually stored in the control unit's memory. Such telephone-specific parameters include telephone number, tariff data relating to the calls to be placed, language options on the telephone's display and volume of voice. Except for the inventive features described in the present application, the operation of the control unit does not basically differ from the operation of the control units of prior art pay phones.

The details of the terminal structure can also vary from the above description depending on the purpose of use of the terminal. For example, if the terminal is a payment terminal used at a point of sale, the device does not necessarily include audio parts such as a microphone or speaker. At its simplest, the terminal comprises a cellular radio transceiver, a control unit and collection means which can be structurally integrated with each other or, alternatively, they may be components detachable from one another and temporarily connected together for the duration of a call payment or a purchase transaction, for example.

The software needed by the terminal are stored into the memory of a control unit 204. The software concerned include software, or card applications, needed by various payment card alternatives. A card application comprises routines needed for the terminal's user interface, for controlling a card and for carrying out a card transaction, such as a payment.

Let us then study the method of the invention with reference to a flow diagram shown in Figure 3. As stated above, the system of the invention allows software to be downloaded to terminals, when necessary, from the system server. To ensure the authenticity of the software it is important that software can only be uploaded to the server from a source the authenticity of which has been confirmed. In the solution of the invention, each software supplier is therefore provided with a specific digital certificate that allows the software supplier, or the supplier's computer (hereinafter referred to as the source computer) from which the software is uploaded to the server, to be identified. The certificate is granted by a third party, such as the terminal manufacturer.

In step 300 of Figure 3, the software producer attaches a digital certificate confirming the authenticity of the software to the software to be

transferred to a server. In step 302 the software is uploaded from the software producer's source computer via, for example, the Internet or another link to the network server which in this example is the server of the pay phone system. In a preferred embodiment of the invention, the server checks the source computer's certificate in connection with the downloading.

When software is downloaded to terminals, it is also essential that the software is downloaded from an official server agreed on in advance and not from a disturber that has connected to the network. It is therefore necessary that the origin of the software can be verified from the software. For this purpose the software is provided with an electronic signature at the server, the signature being attached to the software in step 306. In the preferred embodiment of the invention, the electronic signature is generated by calculating a check sum in step 304 for the software and the certificate and by attaching the check sum to the software in step 306, preferably by using encryption, thereby preventing any external party from corrupting the sum. The check sum itself can be calculated by applying methods known to those skilled in the art. One way of implementing the encryption is to use a public key and secret key encryption method. The electronic signature is attached to the software at the server in step 306 by using the server's secret key which outsiders do not know. The encrypted information can then be decrypted by using a public key at the terminal. In the solution of the invention, encryption methods known to those skilled in the art can be used.

In step 308 the terminal downloads the software needed from the server. After the terminal has downloaded the software, it checks the authenticity of the software in step 310 by calculating, similarly as at the server, the check sum of the downloaded software and the certificate attached to the software. The terminal then decrypts the encrypted electronic signature attached to the software at the server in step 312 by using the server's public key. As a result of the decryption, the check sum calculated at the server is obtained. The terminal compares the check sum it has calculated with that calculated at the server in step 314, the result of the comparison allowing the terminal to decide the authenticity. If the check sums match, the software is authentic (step 316), but if the check sums do not match, the source of the software is not authentic (step 318) and the software cannot be taken into use.

Let us then study an example of a situation where the above described downloading of the software cannot be carried out; this is illustrated

in a flow diagram of Figure 4. In step 400 the user has inserted a card into a card reader 206 of a terminal. In step 402 the terminal checks the different functions of the card, for example, any credit card alternatives included. If several options are available, the user gets to select the function to be used. The routine then proceeds to step 406 to check whether an application required by the selected function is included in the terminal's memory. The application keeps record of the applications available in its memory at a particular moment. If the application is in the memory, it can be started in step 408.

If the application is not in the terminal's memory, the routine proceeds to step 410 to check whether the application is in the management system's server. Information about the applications that can be downloaded from the server can be stored either in the terminal, or the terminal can request the information from the server. If the application cannot be found from the management system, the function is rejected in step 412 and the user is asked to give a new one, provided that the card contains several functions.

If the application is on the management system's server, the terminal asks in step 414 the amount of memory required by the application. The terminal then checks in step 416 whether the amount of memory required by the application is available. If there is not enough memory available, an application to be removed from the memory is selected and removed in step 418 so as to release memory for the new application. The terminal can let the user select the application to be removed or, alternatively, the terminal can make the decision on the basis of a predetermined criterion. One criterion is to keep recently used applications and to remove an application that has been unused for the longest.

The terminal then informs in step 420 the server of a free memory area where the application should be placed. For example, the terminal can inform a memory area 312, shown in Figure 3, to be available for the application. The management system's server downloads in step 422 the application to the memory area informed by the terminal. The application is then ready to be taken into use in step 424.

In another alternative embodiment the management system's server does not control the placing of the application into the terminal's memory, but only transmits the application to the terminal which then places the application into its memory.

In addition to payment card applications, a downloadable software can comprise facilities transferred in an electronic form, such as timetable information or tickets.

Method steps associated with the terminal of the invention can be advantageously implemented by software at the terminal's control unit 204. The connection to the management system's server required by the method can be advantageously provided by means of a data call connection. A data call is a call type that is available in digital radio networks; it corresponds to a modem connection in analog systems.

At the management system's server and in the software manufacturer's source computer the functions of the invention can be advantageously implemented by means of software.

Although the invention is described above with reference to an example shown in the attached drawings, it is apparent that the invention is not restricted to it, but can vary in many ways within the inventive idea disclosed in the attached claims.

4. CLAIMS

1. A method for downloading software from a server (128) to a terminal (100, 102), the method comprising the steps of

attaching to the software a certificate confirming the authenticity of the software manufacturer and the loader;

uploading the software from a source computer (134) to the server (128);

calculating a check sum for the software and the certificate; and

downloading the software from the server (128) to the terminal (100, 102),

characterized in that the method further comprises the steps of

attaching the check sum confirming the authenticity of the software to the software at the server (128) before the software is downloaded to terminals;

generating a second check sum at the terminal from the downloaded software, after the software has been downloaded; and

checking the authenticity of the software at the terminal by comparing the first check sum with the second.

2. A method according to claim 1, **characterized** in that the authenticity of the software is always checked at the terminal (100, 102) when the software is carried out.

3. A method according to claim 1, **characterized** in that the method comprises the generating of an electronic signature at the server (128) by calculating for the software and the certificate a common check sum which is encrypted by means of a secret key of the server.

4. A method according to claim 3, **characterized** in that the encryption of the secret key is decrypted at the terminal (100, 102) by means of a public key of the server (128).

5. A method according to claim 1, **characterized** in that the terminal (100, 102) detects that a payment card is inserted into the terminal's card reader (206) and the user has selected an application, and that the terminal

checks whether the software needed for implementing the application can be found in the terminal's memory, and

sends the server (128) a loading request comprising information about the software needed, and that the server

sends the terminal the software needed, and that the terminal

stores the software into its memory.

6. A telephone system comprising

a plural number of terminals (100, 102) and

a server (128) monitoring and controlling the operation of the terminals, the server (128) being arranged to calculate a check sum for software and for a certificate attached to the software;

a terminal of the telephone system comprising means (204) for storing one or more software, and the system comprising

one or more source computers (134) arranged to upload software to the server, the terminals (100, 102) being arranged to download software from the server,

characterized in that

the server is arranged to attach to the software a first check sum confirming the authenticity of the software before the software is downloaded to the terminals, and that

a terminal is arranged to generate a second check sum from the downloaded software, after the software has been loaded, and that the terminal is arranged to check the authenticity of the software by comparing the first check sum with the second.

7. A system according to claim 6, **characterized** in that the terminal is arranged to always check the authenticity of the software when the software is carried out.

8. A system according to claim 6, **characterized** in that the server is arranged to generate an electronic signature by calculating for the software and the certificate a common check sum and to encrypt the calculated check sum by means of a secret key of the server.

9. A system according to claim 6, **characterized** in that the terminal is arranged to decrypt the encryption of the electronic signature by means of a public key of the server.

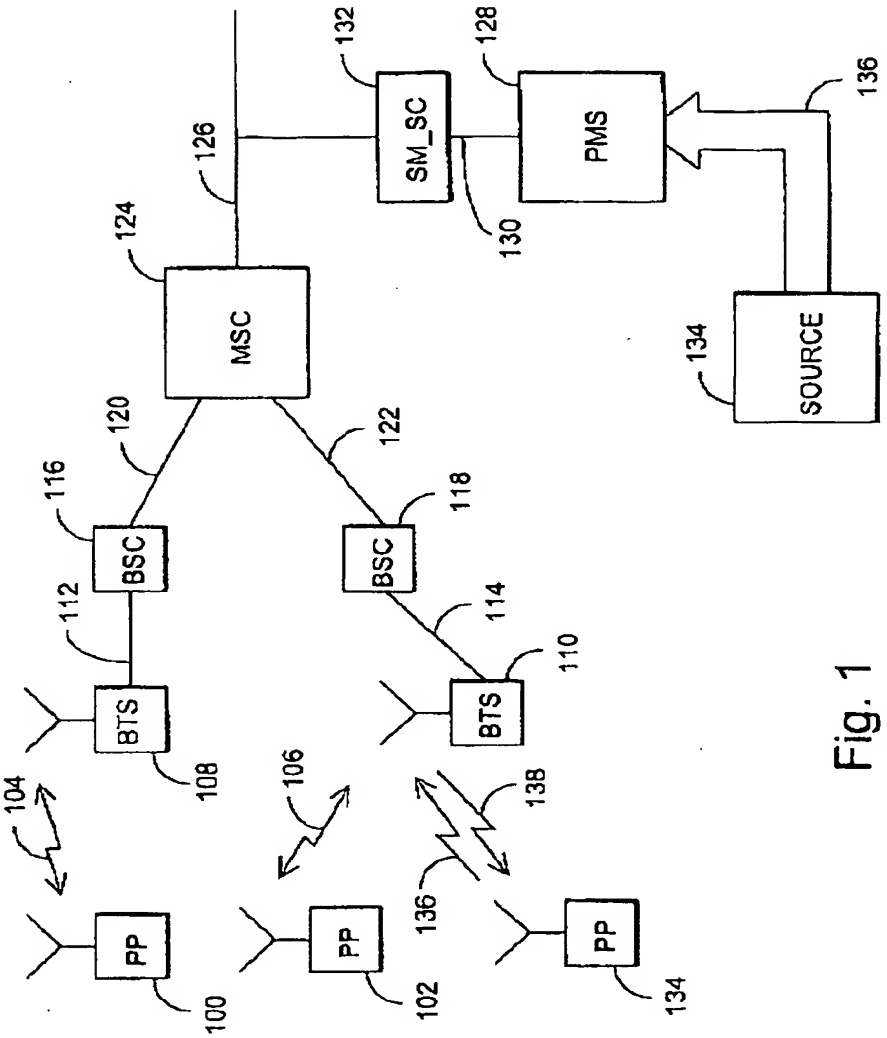

132
128
136
SM_SC
PMS
126
130
124
MSC
SOURCE
134
120
122
116
118
BSC
BSC
112
114
110
BTS
BTS
104
106
108
138
136
PP
PP
PP
100
102
134

Fig. 1

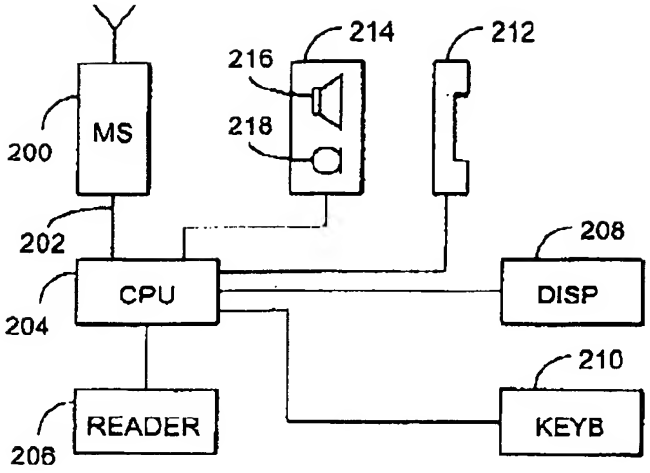


Fig. 2

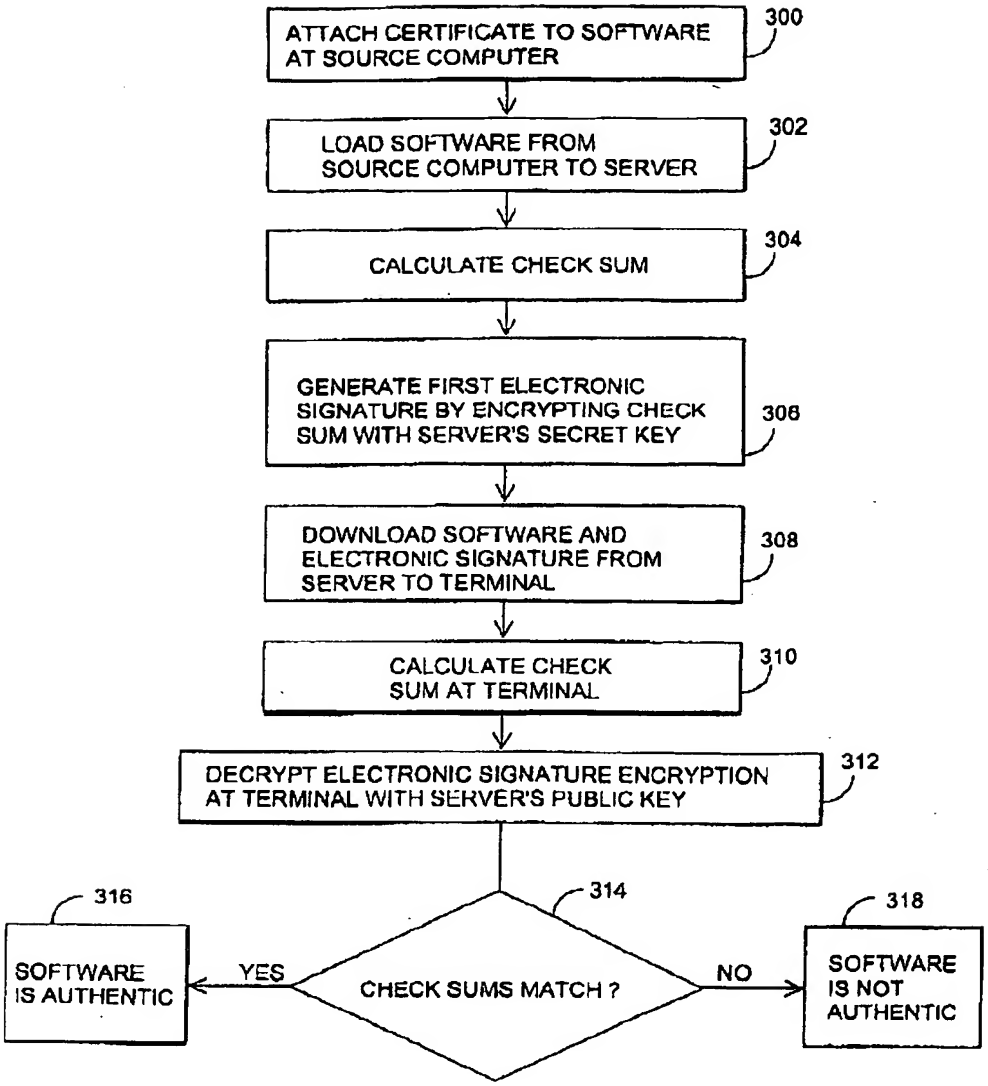

ATTACH CERTIFICATE TO SOFTWARE AT SOURCE COMPUTER
300
LOAD SOFTWARE FROM SOURCE COMPUTER TO SERVER
302
CALCULATE CHECK SUM
304
GENERATE FIRST ELECTRONIC SIGNATURE BY ENCRYPTING CHECK SUM WITH SERVER'S SECRET KEY
306
DOWNLOAD SOFTWARE AND ELECTRONIC SIGNATURE FROM SERVER TO TERMINAL
308
CALCULATE CHECK SUM AT TERMINAL
310
DECRYPT ELECTRONIC SIGNATURE ENCRYPTION AT TERMINAL WITH SERVER'S PUBLIC KEY
312
CHECK SUMS MATCH ?
314
YES
NO
SOFTWARE IS AUTHENTIC
316
SOFTWARE IS NOT AUTHENTIC
318

Fig. 3

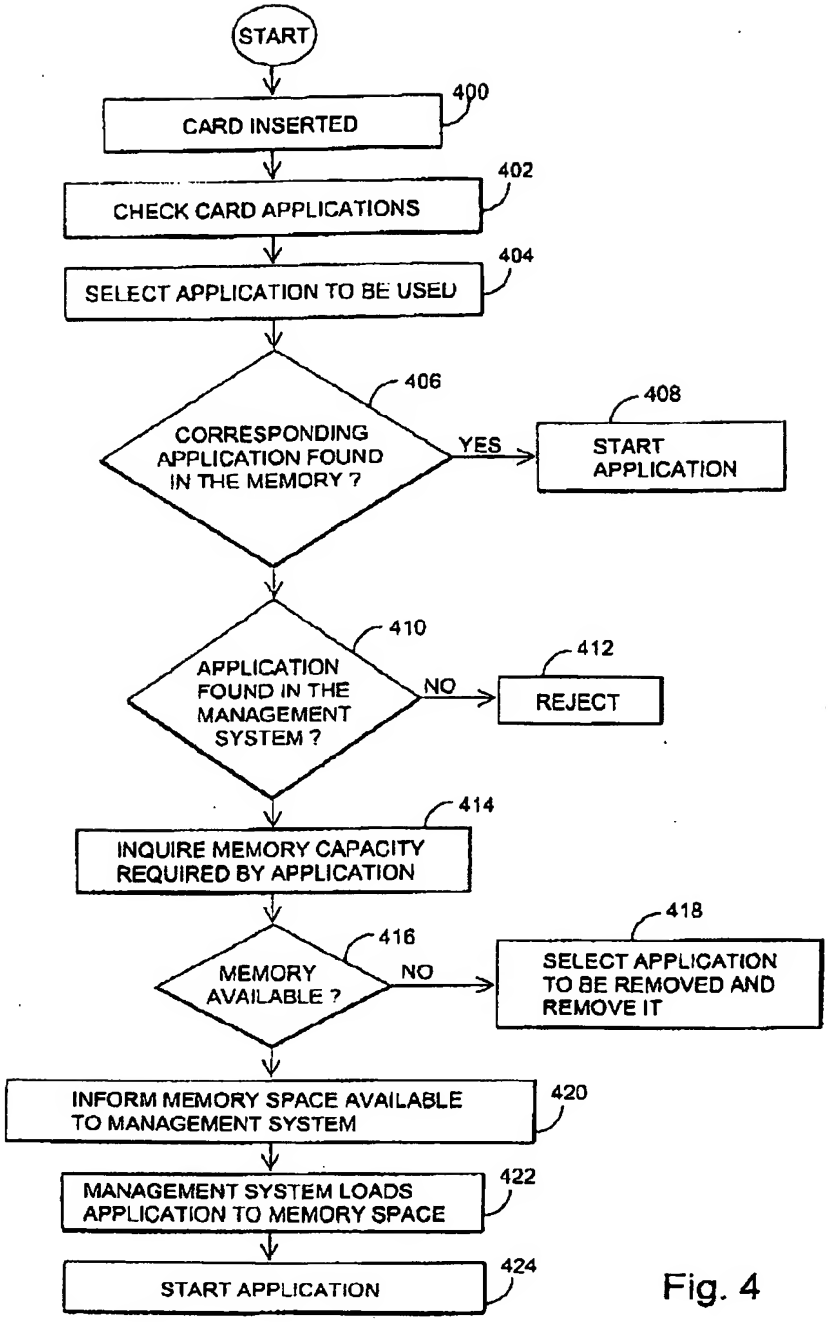

START
CARD INSERTED
400
CHECK CARD APPLICATIONS
402
SELECT APPLICATION TO BE USED
404
CORRESPONDING APPLICATION FOUND IN THE MEMORY ?
406
YES
START APPLICATION
408
APPLICATION FOUND IN THE MANAGEMENT SYSTEM ?
410
NO
REJECT
412
INQUIRE MEMORY CAPACITY REQUIRED BY APPLICATION
414
MEMORY AVAILABLE ?
416
NO
SELECT APPLICATION TO BE REMOVED AND REMOVE IT
418
INFORM MEMORY SPACE AVAILABLE TO MANAGEMENT SYSTEM
420
MANAGEMENT SYSTEM LOADS APPLICATION TO MEMORY SPACE
422
START APPLICATION
424

Fig. 4

1. ABSTRACT

The invention relates to a telephone system and a method for downloading software from a server (128) to a terminal (100, 102), the method comprising the steps of attaching to the software a certificate confirming the authenticity of the software and the loader; downloading the software from a source computer (134) to the server (128); downloading the software from the server (128) to the terminal (100, 102). In the method of the invention a first electronic signature confirming the authenticity of the software is attached to the software at the server (128). After the software is downloaded, a second electronic signature is generated at the terminal from the loaded software and the authenticity of the software is checked by comparing the first electronic signature with the second.

2. REPRESENTATIVE DRAWING

Figure 1